

Auditoria e Análise de Segurança da Informação

Segurança Física e Lógica

Segurança Física e Segurança Lógica da Informação

Segurança Física

A segurança física tem como objetivo proteger equipamentos e informações contra usuários não autorizados, prevenindo o acesso a esses recursos.

A segurança física deve se basear em perímetros predefinidos nas imediações dos recursos computacionais, podendo ser explícita como uma sala-cofre, ou implícita, como áreas de acesso restrito.

Segurança Física

A segurança física pode ser abordada sob duas formas:

- **Segurança de acesso** - trata das medidas de proteção contra o acesso físico não autorizado;
- **Segurança ambiental** – trata da prevenção de danos por causas naturais.

Recomendações para o controle do acesso físico

Deve-se instituir formas de identificação capazes de distinguir funcionários de visitantes e categorias diferenciadas de funcionários, se for o caso.

Solicitar a devolução de bens de propriedade da empresa (crachás, chaves, etc), quando o visitante se retira ou quando o funcionário é retirado de suas funções.

Recomendações para o controle do acesso físico

Controle de entrada e saída de materiais, equipamentos, pessoal, etc, registrando a data, horários e responsável.

No caso de visitantes, restringir a circulação destes nas dependências da empresa e, se necessário, acompanhá-los até o local de destino.

Instalar sistemas de proteção e vigilância 24 x 7.

Recomendações para o controle do acesso físico

Supervisionar a atuação de equipes terceirizadas (limpeza, manutenção predial, vigilância, etc).

Não instalar em áreas de acesso público equipamentos que permitam o acesso à rede interna da corporação.

Orientar os funcionários para que não deixem ligados computadores sem a devida supervisão, principalmente no horário das refeições ou quando se ausentarem por tempo prolongado.

Recomendações para o controle do acesso físico

Utilizar mecanismos de controle de acesso físico em salas e áreas de acesso restrito (fechaduras eletrônicas, câmeras de vídeo, alarmes, etc);

Proteger as linhas telefônicas internas e externas com dispositivos contra “grampos”

Proteger fisicamente as unidades de backup e restringir o acesso a computadores e impressoras que possam conter dados confidenciais.

Política de Segurança Física

A política e o investimento no controle de acesso físico adotada pela empresa estará diretamente ligada à importância de seus ativos, observando sempre a relação dos modelos de segurança do que apenas o uso de tecnologia.

É fundamental a análise do perfil da empresa para definir a política de controle de acesso físico que se encaixe nas necessidades dos usuários.

Política de Segurança Física

Quanto maior o investimento em prevenção menor será o prejuízo em caso de Sinistro.

O investimento não se refere apenas ao uso de tecnologia avançada, mas à forma como a empresa lida com a conscientização de seus funcionários.

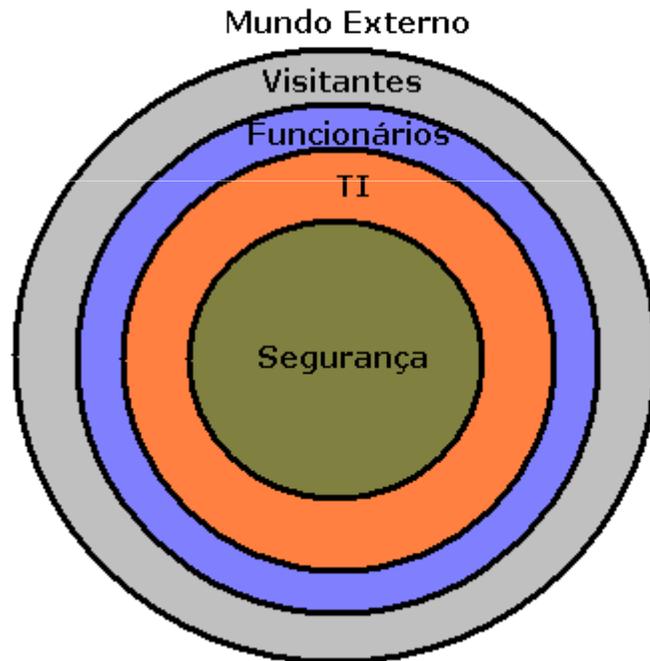
Política de Segurança Física

Itens de avaliação para riscos:

- **Incêndios;**
- **Treinamento de pessoal;**
- **Danos pela água;**
- **Climatização;**
- **Eletricidade;**
- **Controle de acesso.**

Política de Segurança Física

Solução em níveis ou “Modelo da cebola”.



Mundo Externo – Área não-controlada ao redor das instalações;

Visitantes – Área de espera para entrada de visitantes;

Funcionários – Área de funções comerciais normais;

TI – Materiais e equipamentos críticos à atividade comercial.

Segurança Lógica

A segurança lógica é um processo em que um sujeito ativo deseja acessar um objeto passivo.

O sujeito é um usuário ou um processo da rede e o objeto pode ser um arquivo ou outro recurso de rede (estação de trabalho, impressora, etc).

Segurança Lógica

A segurança lógica compreende um conjunto de medida e procedimentos, adotados pela empresa ou intrínsecos aos sistemas utilizados.

O objetivo é proteger os dados, programas e sistemas contra tentativas de acessos não autorizados, feitas por usuários ou outros programas.

Segurança Lógica

Recursos e informações a serem protegidos:

- **Aplicativos (Programas fonte e objeto);**
- **Arquivos de dados;**
- **Utilitários e Sistema Operacional;**
- **Arquivos de senha;**
- **Arquivos de log;**

Segurança Lógica

O controle de acesso lógico pode ser visualizado de dois modos diferentes:

- **A partir do recurso computacional que se pretende proteger;**
- **A partir do usuário a quem se pretende dar privilégios e acesso aos recursos.**

Segurança Lógica

A proteção dos recursos computacionais baseia-se na necessidade de acesso de cada usuário.

A identificação e autenticação do usuário é feita normalmente por uma identificação (userID) e uma senha durante o processo de logon.



Segurança Lógica

Elementos básicos de controle do acesso lógico:

- **Apenas usuários autorizados devem ter acesso aos recursos computacionais;**
- **Os usuários devem ter acesso apenas aos recursos realmente necessários para a execução de suas tarefas;**
- **O acesso aos recursos críticos do sistema deve ser monitorado e restrito;**
- **Os usuários não podem executar transações incompatíveis com sua função.**